HIRSCHMANN
A Belden Company

WLAN Outdoor Guide

Technical Support
HAC-Support@hirschmann.de

Windows®, Windows Vista™, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp. LCOS is registered trademarks of LANCOM Systems GmbH.
The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2008 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit http://www.openssl.org/.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (30.6.2008)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538

Content

1 Preface **5**

2 Introduction **7**

2.1 Application scenarios 7
2.1.1 Campus coverage 7
2.1.2 Hotspot 8
2.1.3 Data transfer to mobile objects in industrial environments. 8
2.1.4 Wireless link (point-to-point) 9
2.1.5 Wireless Distribution System (point-to-multipoint) 10
2.1.6 Wireless links in relay mode 11

2.2 Components of the wireless LAN system 11
2.2.1 access points and Wireless router 11
2.2.2 Power supply to the access point 12
2.2.3 External antennas 12
2.2.4 Lightning and surge protection equipment 14

3 Point-to-point connections **15**

3.1 Geometric dimensioning 16

3.2 Antenna alignment 19

4 Lightning and surge protection **22**

4.1 Where do lightning discharges come from? 22

4.2 External lightning protection 24

4.3 Internal lightning protection 25
4.3.1 Selecting the lightning and surge protective components 26
4.3.2 Example applications 29

5 Installation **33**

5.1 Safety advice 33

5.2 Mounting the access points 34
5.2.1 Selecting where to mount 34
5.2.2 Wall mounting 35
5.2.3 Pole mounting 35
5.3 Mounting antennas 36
5.3.1 Selecting where to mount 36
5.3.2 Wall mounting 37
5.3.3 Mast mounting 37
5.4 Mounting the lightning rods 38
5.4.1 Dimensioning of the lightning rod 38
5.4.2 Distance to the components at risk 38
5.4.3 Lightning charge conduction (grounding) 39

6 Appendix 40
6.1 Antenna gain, EIRP and antenna radiation characteristics 40
6.2 Selecting the frequency band 45
6.2.1 2.4 or 5 GHz band 45
6.2.2 Special regulations for the 5 GHz band 46

7 Index 50

1 Preface

The advantages of wireless LANsre are obvious – they offer flexibility, mobility and convenience at a lower cost than cabled networks. WLANs can be quickly installed without any changes to the building's construction, and they offer new applications not available with cabled LANs. BAT wireless routers and BAT access points combine with appropriate antennas for establishing wireless LANs both indoors and outdoors.
BAT wireless routerBAT access pointThis document applies for all BAT wireless routers and BAT access points in combination with antennas of the BAT product line and it provides general information on the outdoor operation of wireless LAN systems. Information on the installation and basic configuration of the various wireless routers, access points and antennas is available from the corresponding user manual.

Danger: Protecting the components employed from the consequences of lightning strikes and other electrostatic influences is one of the most important aspects to be considered when designing and installing wireless LAN systems for outdoor use. Please refer to the appropriate notes in Chapter →'Lightning and surge protection' as otherwise Hirschmann cannot provide any guarantee for damage to BAT components.

The reference manual can be found on the product CD as an Acrobat (PDF) document. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of models.

Danger: Safety notices: safety notices concerning the mounting and installation of wireless LAN system components are to be found at relevant locations in the following chapters.

This documentation was created by ...

... several members of our staff from a variety of departments in order to ensure you the best possible support when using your BAT product.
In case you encounter any errors, or just want to issue critics enhancements, please do not hesitate to send an email directly to:
info@hirschmann.com

Note: Our online services www.hirschmann.com are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.
In addition, BAT support is available. For telephone numbers and contact addresses of BAT support, please see the enclosed leaflet or the Hirschmann website.

2 Introduction

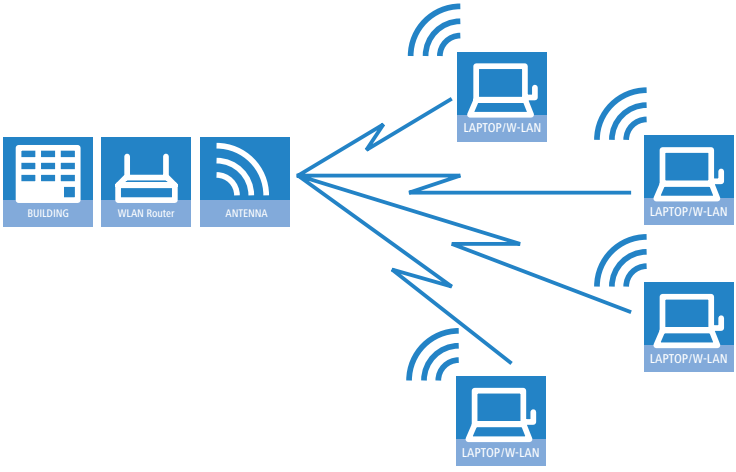
This chapter presents the basic application scenarios for wireless LAN outdoor systems. These include, for example campus coverage, industrial applications and wireless links. We also list the components required to set up a wireless LAN system outdoors.

2.1 Application scenarios

Wireless LAN systems can act as an extension to or even as a replacement for cabled networks. In some cases wireless LANs even provide completely new application possibilities, which can mean a major advance in the way work is organized, or significant cost savings.

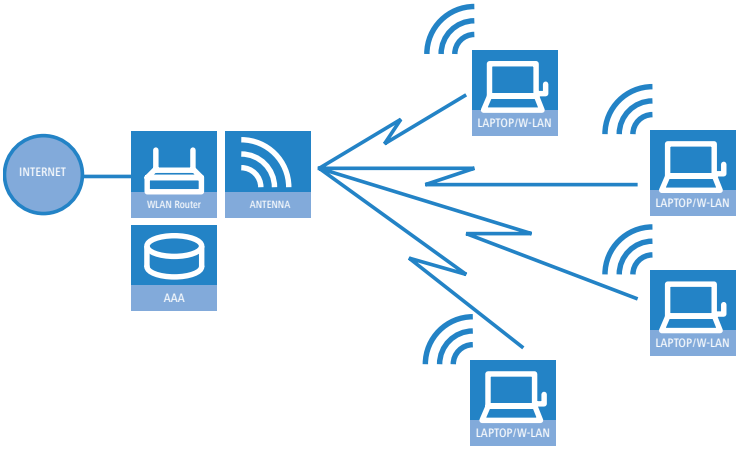
2.1.1 Campus coverage

Coverage for campuses is provided by wireless LAN system antennas mounted on building facades or on special mountings or masts. In this way radio cells cover the open areas, and all wireless LAN clients with the appropriate rights have access to the network. A common term used here is "campus coverage" because this solution is used by a large number of colleges and universities to provide students and staff with network access.



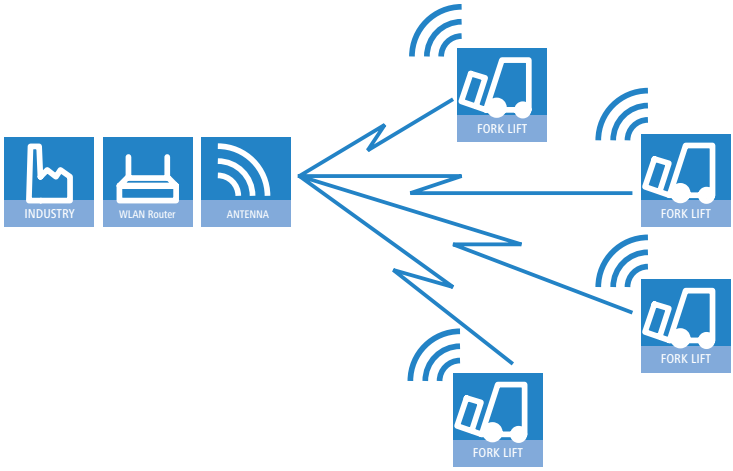
2.1.2 Hotspot

A hotspot is a special variant of the campus coverage described above. Whereas campus coverage provides the members of a closed user group with access to a network that includes all the necessary services (often at no charge), a hotspot provides network access (generally restricted to Internet only) to wireless LAN clients at a fee. In addition to the differences in access point configuration, setting up a hotspot requires authentication, authorization and accounting (AAA) functions such as those provided by e.g. Public Spot options Hotspots are generally set up at public locations where people have a short-term need to access the Internet, such as at airports, cafés or hotels.



2.1.3 Data transfer to mobile objects in industrial environments.

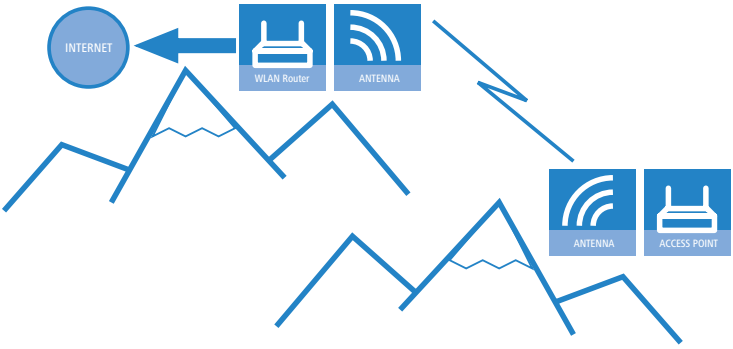
Completely new applications allow wireless LAN systems in industrial environments to transmit data to mobile objects. In logistics, for example, this means that fork-lift trucks can stay continuously connected to the company network via the wireless LAN. In combination with mobile barcode scanners, inventory movements within a warehouse can be monitored in real time and passed on to an ERP system, which then provides all employees with up-to-the-minute information on current inventories at all times.



2.1.4 Wireless link (point-to-point)

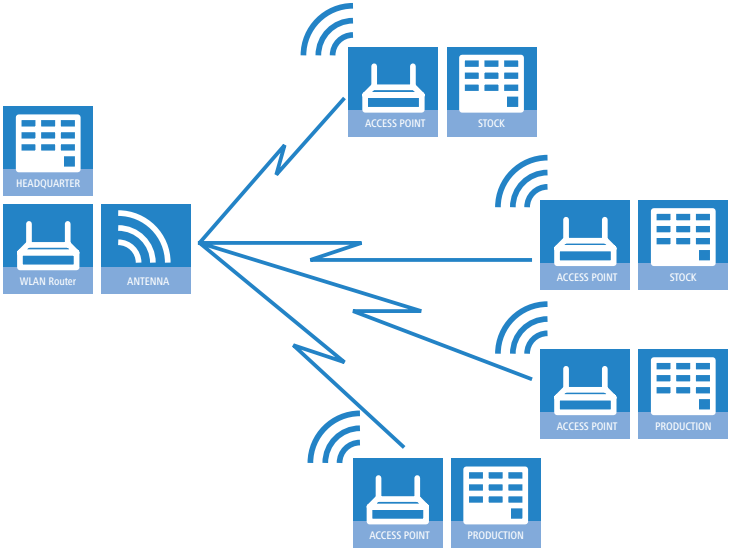
Whereas the scenarios discussed so far have involved connecting multiple WLAN clients to one access point (point-to-multipoint), outdoor wireless LAN systems are particularly advantageous for providing a link between two access points (point to point). By setting up a wireless link between two access points, a distant production building on extensive company premises can be very easily integrated into the company network, for example.

A point-to-point connection can also be used in difficult ter rain (such as mountainous areas or islands) to provide Internet access in areas where cabling would be too expensive. With a good line of sight between the two access points, distances of several kilometers can be bridged by this type of wireless link.



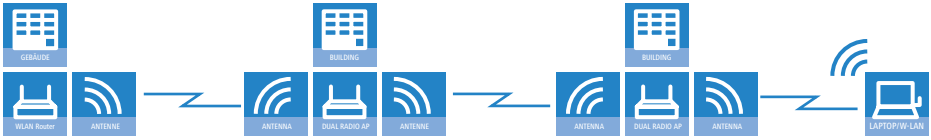
2.1.5 Wireless Distribution System (point-to-multipoint)

A special type of wireless link is the connection of several distributed access points to a central point – the point-to-multipoint wireless LAN (P2MP) is also referred to as a Wireless Distribution System (WDS). This mode of operation allows for example several buildings on a company's premises to be connected to the central administrative building. The central access point or Wireless router is configured as "master" and the remote WDS stations as "slaves".



2.1.6 Wireless links in relay mode

In some cases, the distance between the access points for connection exceeds the range of a single wireless link. This may be the case when the distance between the access points exceeds the radio range, or when obstacles exist in the line of site between the two access points
In these cases, the two end points can be connected by stringing together multiple access points, each of which has two WLAN modules. Because the intermediate access points often operate solely as relay stations, the operating mode of these access points is referred to as "relay mode".



Although BAT access points can run several P2P links simultaneously on each wireless module in addition to supporting wireless LAN clients, we recommended the use of BAT access points with two wireless modules for performance reasons.

2.2 Components of the wireless LAN system

Generally speaking a WLAN system consists of the following components, some of which are optional.

2.2.1 access points and Wireless router

Hirschmann supplies access points and Wireless routers for various applications. access points are generally used to establish wireless LAN networks (SSIDs) or wireless links (P2P), whereas Wireless routers also provide full router functionality including a WAN interface and further optional functions such as VPN, etc.
Along with classification into access points and Wireless routers, the following characteristics are also important when considering the use of wireless LAN devices.

- Environmental conditions: The various models may be suitable for operation in an office environment only or, alternatively, for tougher conditions such as those found in logistics warehouses. A third group has been designed for operation under extreme weather conditions, i.e. water resistant, and some are for operation in extreme temperatures.
- Standards supported: Depending on model type, the access points support the following standards: IEEE 802.11a (5 GHz band), IEEE 802.11b or IEEE 802.11g (2.4 GHz band) or IEEE 802.11n (2.4 and 5 GHz bands). While the 5 GHz band is highly suited to directional radio links due to the higher performance, models in the 2.4 GHz band are more suitable for connecting mobile clients.

Note: Please refer to the appendix in this manual for more information on the frequency bands and their permitted use in different countries.

- Number of wireless LAN modules: Devices can be fitted with two wireless LAN modules and used as relays for directional radio links over distances that exceed the range of a single P2P connection.

2.2.2 Power supply to the access point

An alternative to supplying power to an access point via its own internal power adapter is to use Power over Ethernet (PoE). PoE-capable network devices can be neatly provided with power over LAN cabling. A power supply for each access point is therefore not necessary, significantly reducing the effort of installation.
Power is fed into the LAN at a central location by using a PoE injector, a power hub or power switch. It is important that all eight wires are connected in the LAN cabling.

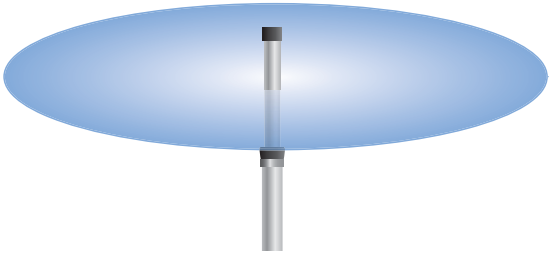
Caution: PoE injectors available on the market support different standards and technical specifications depending on the model. Please ensure that the PoE injector is suitable for the access point being used.

2.2.3 External antennas

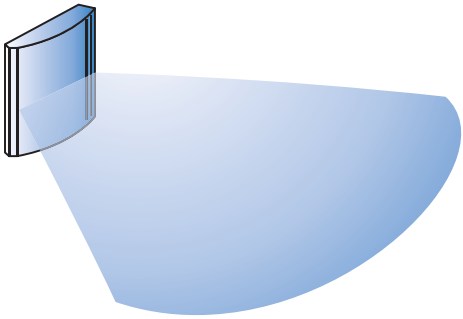
Most BAT access points are supplied with an antenna. However, for many of the outdoor applications relevant to this documentation, additional external antennas are necessary to meet the specialized demands. The following sections contain a brief description of the different types of antenna:

Note: Please refer to the appendix in this manual for more information on the typical antenna characteristics of antenna gain, EIRP and radiation patterns.

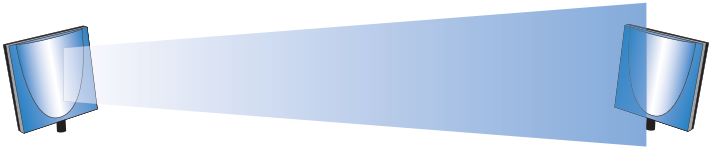
- Omnidirectional antennas transmit horizontally with equal power in all directions. They have very limited vertical spread, which determines the antenna gain. Antennas of this type are typically located in the center of open spaces or larger offices to provide even coverage to all clients.



- Sector antennas have beams with fairly wide horizontal and vertical angles, for example between 60° and 90°. Sector antennas are generally mounted on the wall of a building or in the corner of a room to provide an even coverage—often referred to as "campus coverage".



- Directional antennas have beams with narrow horizontal and vertical angles, for example of 9°. Directional antennas are mainly used on rooftops or masts for establishing point-to-point links that interconnect areas of a network that are separated by a distance.



- Polarization diversity antennas (antenna diversity)

The transmission of radio signals can suffer from, among other things, significant signal losses due to reflection and scatter . When electromagnetic waves overlap at the point of reception, the strength of the signals may be reduced or completely obliterated (interference). Transmission quality can be improved with so-called "diversity" methods.
The polarization diversity method makes use of the electromagnetic polarization of the radio waves. The transmitter broadcasts the wireless LAN signals as linearly polarized waves with a fixed direction of polarization. The polarization may be modified over the radio link by reflection and diffraction so that signals reach the receiver with differing polarization. Polarization diversity antennas use two signals with polarization turned through 90°. The two antenna signals result in genuinely improved performance with conventional diversity antennas since the stronger of the two signals can be used.
MIMO technology (multiple input, multiple output) used in wireless LAN standard 802.11n goes a step further. These multiple receivers and transmitters can use the horizontally and vertically polarized waves as independent transmission paths and thus transmit double the amount of data on one frequency.
Two antennas are connected to the access point's main and auxiliary ports in order to receive both signals.

Note: For further information on the subject of 'Polarization diversity antennas (antenna diversity)' refer to the LCOS reference manual.

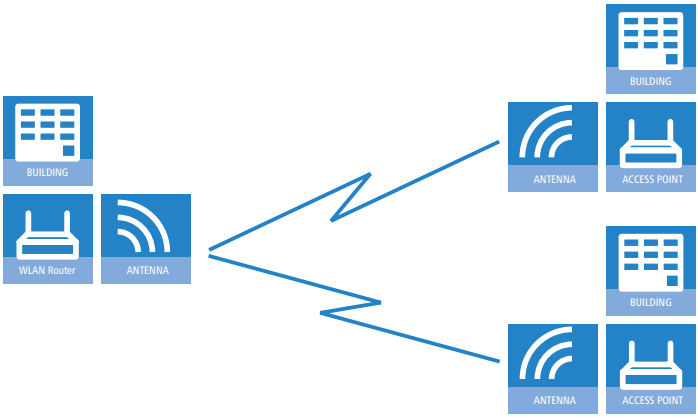
2.2.4 Lightning and surge protection equipment

Besides the central components (access point, antenna and power supply) the most important accessories in a wireless LAN system are those for lightning and power surge protection. Lightning and other electrostatic occurrences in the atmosphere can impinge on the wireless LAN system in different ways and cause harm to people, machines and equipment. The lightning and surge protection components guard against the effects of electrostatic discharge or reduce the surges to a level that is harmless for people and equipment.

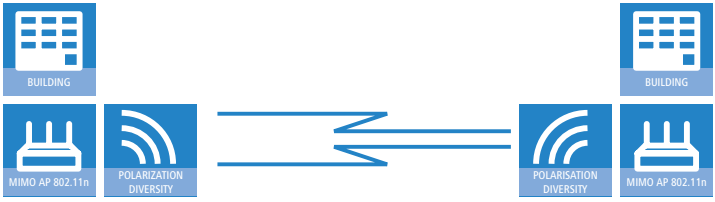
Note: Please refer to Chapter → 'Lightning and surge protection'.

3 Point-to-point connections

BAT Wireless access points can serve not only as central stations in a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart — without direct cabling or expensive leased lines.



When using access points and appropriately polarized antennas in accordance with IEEE 802.11n two wireless links can be established simultaneously between the end points of a point-to-point connection. This allows higher data throughput to be achieved or greater distances to be covered than when using other standards.



This chapter introduces the basic principles involved in designing point-to-point links and provides tips on aligning the antennas.

Note: Please refer to the appendix of WLAN Outdoor Guide for information on the frequency ranges used. You can find information on configuring the access points in the relevant equipment documentation or in the LCOS reference manual.

3.1 Geometric dimensioning

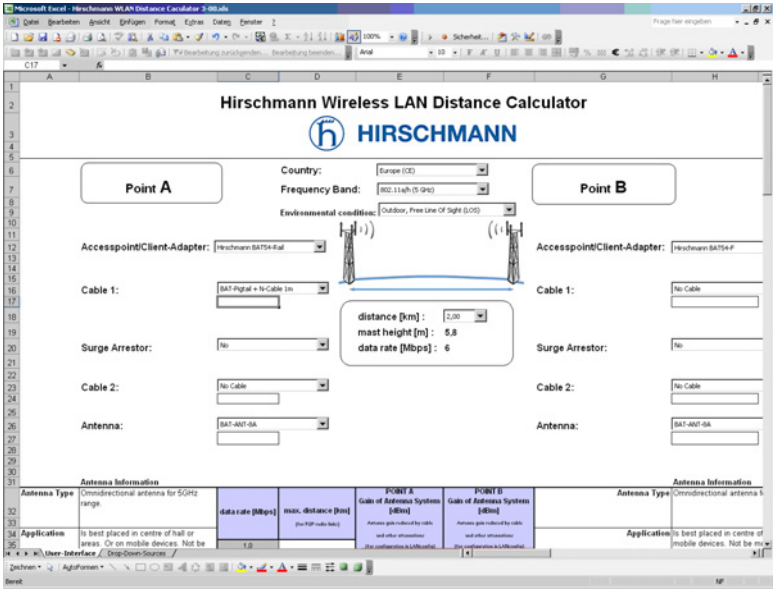
The following basic questions must be answered when designing wireless links:

- What antennas must be used for the desired application?
- How must the antennas be positioned to ensure a problem-free connection?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

Selection of antennas using the BAT Antenna Calculator

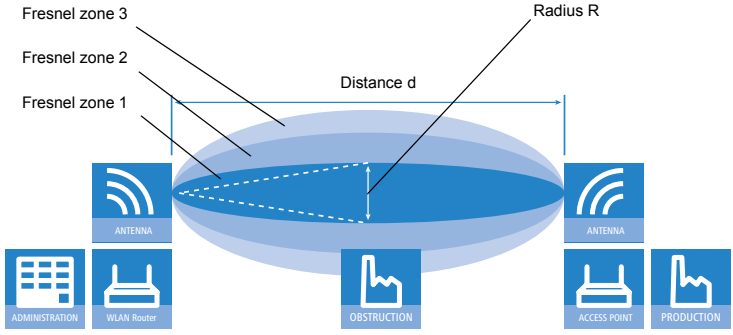
You can use the BAT Antenna Calculator to calculate the output power of the access points as well as the achievable distances and data rates. The program can be downloaded from our website at www.hirschmann.com.
After selecting your components (access points, antennas, lightning protection and cable) the calculator works out the data rates, ranges, and the antenna gain settings that have to be entered into the access point.

Caution: Please note that when using 5 GHz antennas additional technologies such as dynamic frequency selection (DFS) may be stipulated depending on the country of use. The operator of the wireless LAN system is responsible for ensuring that local regulations are met.

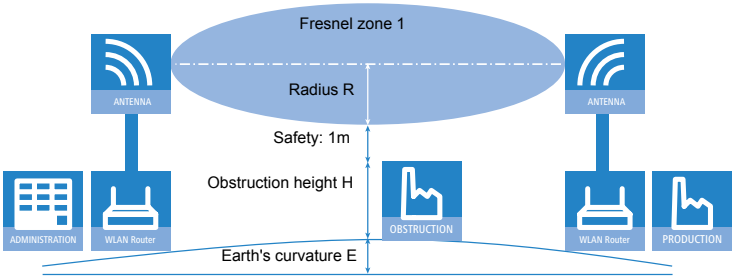


Positioning the antennas

Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves results in amplification of or interference to the effective power output at certain intervals of the connection between the transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



The Fresnel zone 1 must remain free from obstruction in order to ensure that the maximum level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object not only screens off a portion of the Fresnel zone, but the resulting reflections also lead to a significant reduction in signal reception.
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength (λ) and the distance between transmitter and receiver (d) are known.
$R = 0.5 * \sqrt{(\lambda * d)}$
The wavelength in the 2.4 GHz band is approx. 0.125 m, in the 5 GHz band approx. 0.05 m.
Example: With a separating distance of 4 km between the two antennae, the radius of Fresnel zone 1 in the 2.4-GHz band is ***11 m***, in the 5-GHz band ***7 m***.
To ensure that the Fresnel zone 1 remains unobstructed, the height of the antennas must exceed that of the highest obstruction by this radius. The full height of the antenna mast (M) should be as depicted:

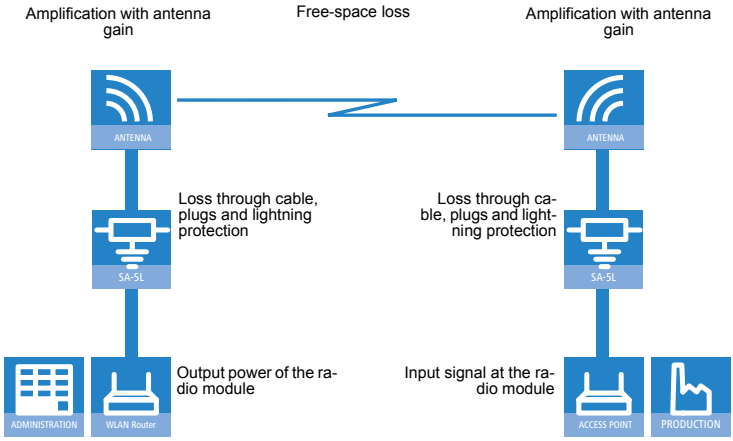


M = R + 1m + H + E (earth's curvature)
The allowance for the curvature of the earth (E) can be calculated at a distance (d) as $E = d^2 * 0.0147$ – i.e. at a distance of 8 km this is almost 1m
Example: With a distance of 8 km between the antennae, the result in the 2.4-GHz band is a mast height above the level of the highest obstruction of approx. ***13 m***, in the 5-GHz band ***9 m***.

Antenna power

The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

The calculation of effective power considers everything from the radio module in the transmitting access point to the radio module in the receiving access point. In between there are attenuating elements such as the cable, plug connections or simply the air transmitting the signals and amplifying elements such as the external antennas.

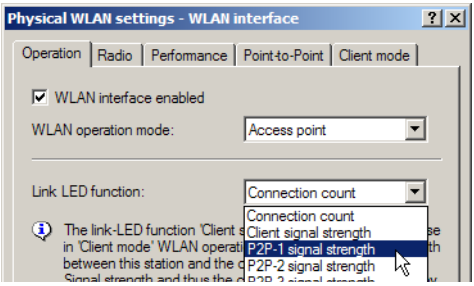


3.2 Antenna alignment

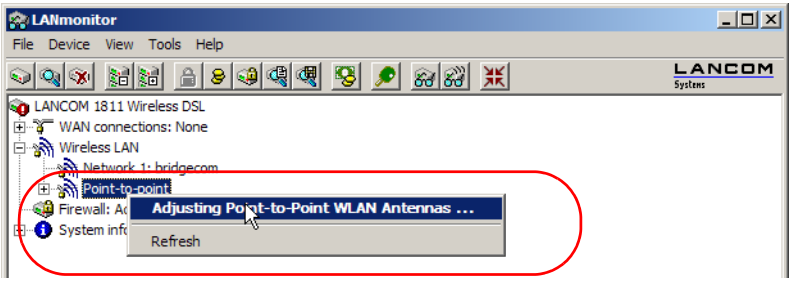
The precise alignment of the antennas is of considerable importance in establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better are the actual performance and the effective bandwidth ❶. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result ❷.

The current signal quality over a P2P connection can be displayed on the device's LEDs or in the LANmonitor in order to help find the best possible alignment for the antennas.

The display of signal quality on the LEDs must be activated for the wireless LAN interface (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation**). The faster the LED blinks the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double the frequency indicates that the signal strength is twice as high).



In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'

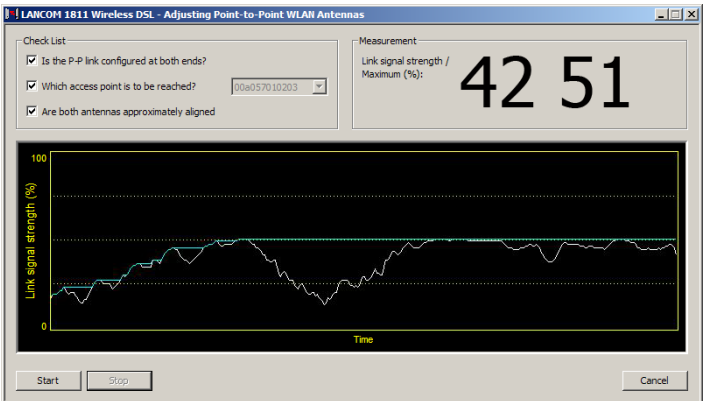


Note: The 'Point-to-point' entry is only visible in the LANmonitor if the monitored device has at least one base station defined as a remote station for a P2P connection (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-Point**).

In the dialog for setting up point-to-point connections, LANmonitor prompts for the information required to establish the P2P connection:

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Is the point-to-point mode of operation activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote stations in the device concerned can be selected here.
- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.

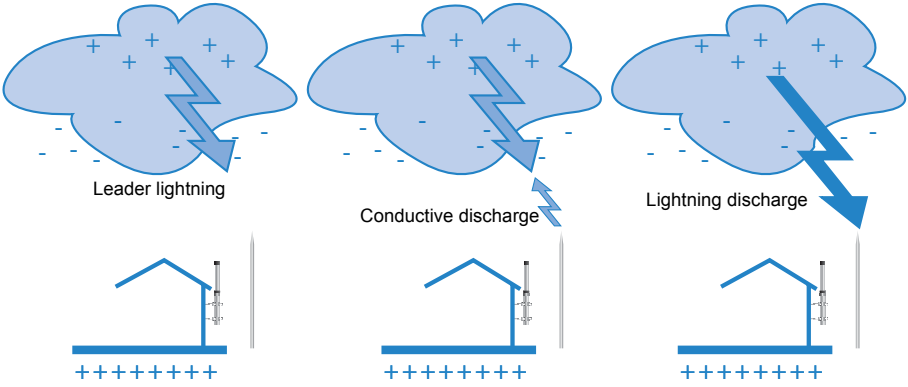


Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

4 Lightning and surge protection

4.1 Where do lightning discharges come from?

Lightning flashes are electromagnetic discharges that are caused by differences in electric potential. Water particles are charged through friction when there is weather movement in the atmosphere. The predominantly positively charged particles rise upwards while the negatively charged particles tend to remain at the lower levels. This uneven distribution of electrical charge can cause discharges within the clouds that can be observed as cloud-to-cloud lightning.



As the earth is predominantly positively charged, a difference between the potential of the cloud and the earth arises. As soon as this potential difference is large enough, leader lightning descends earthwards.

Direct lightning strike

The most frequent type of lightning is cloud-earth lightning. A so-called lightning leader develops from a negatively charged center of a thundercloud. This leader descends, and when it is between 10 m and a several 100 m from the earth the electrical field strength increases so strongly in exposed places – for example at the roof of a house or top of a tree or even the tip of an antenna – that similar and opposite discharges to the lightening leader develop there, the so-called conductive discharges. One of possibly many conductive discharges meets the lightning leader and "earths" it. This determines the point where lightning strikes.
If an antenna is struck by lightning, the instant increase in voltage is conducted via the coaxial cable to any connected devices, i.e. the access points in a wireless LAN system, and this generally results in their destruction. Additionally, any ungrounded components of a wireless LAN system may be subject to sparks or arcing to any earthed metal parts in the vicinity.

Partial discharges

Even if a conductive discharge originates in an antenna it does not necessarily mean that lightning will strike the antenna. In order to feed the conductive discharge in the antenna, a momentary electrical impulse flows through the antenna system – this is called a partial discharge. A partial discharge is therefore a conductive discharge that does not lead to a direct lightning strike. These partial discharges can also result in damage to connected electronic equipment such as access points unless protective measures are taken.

Danger: Even when there are no visible phenomena such as thunderstorms or a direct lightning strike, invisible electrical discharges from the atmosphere can still occur that can lead to sensitive wireless LAN modules or other electronic devices being destroyed or damaged.

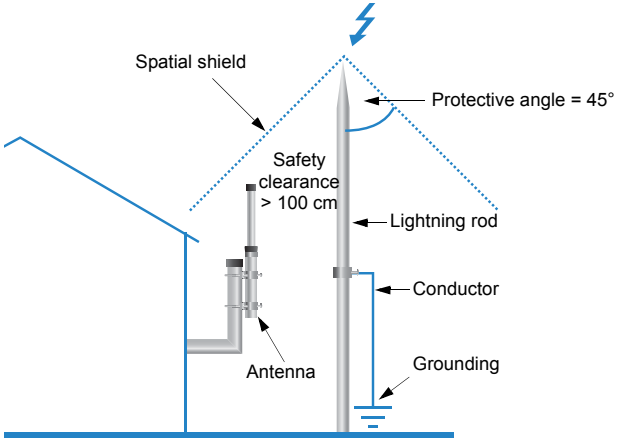
Risks to antennas

Antennas for wireless LAN systems are at particular risk from lightning strike as they tend to be mounted in exposed positions and they are designed to be very good electrical conductors.
The more pointed, needle-shaped and exposed antennas are, the greater the danger posed by a conductive discharge that could result in a direct lightning strike or partial discharge.

Caution: Please note that the explanations of lightning protection in this documentation only refer to protection for wireless LAN systems. The protection of the buildings themselves and other equipment and associated networks (LANs) must be installed and planned separately, if necessary.

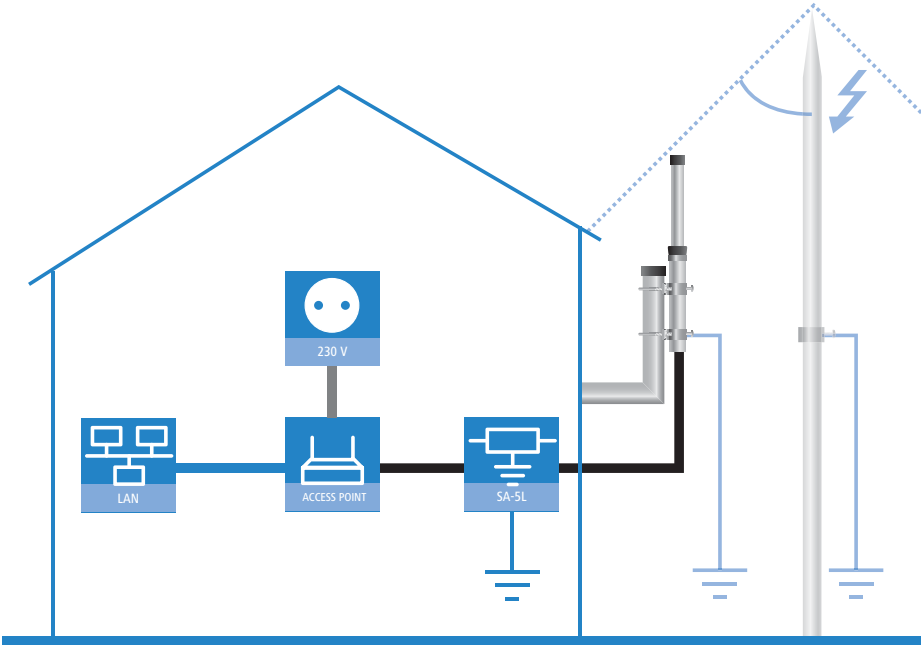
4.2 External lightning protection

External lightning protection includes all measures intended to prevent a ***direct*** lightning strike in the equipment to be protected. This includes, for example, arrester equipment such as lightning rods etc. which intentionally offer an exposed point for electrical discharges. Any lightning striking this equipment is channeled by a conductor along the shortest path to the grounding system. Intentionally "catching" the lightning with the arresting equipment creates a spatial shield where no direct lightning strike is possible. The actual design and construction of external lightning protection depends on the prevailing structural circumstances.

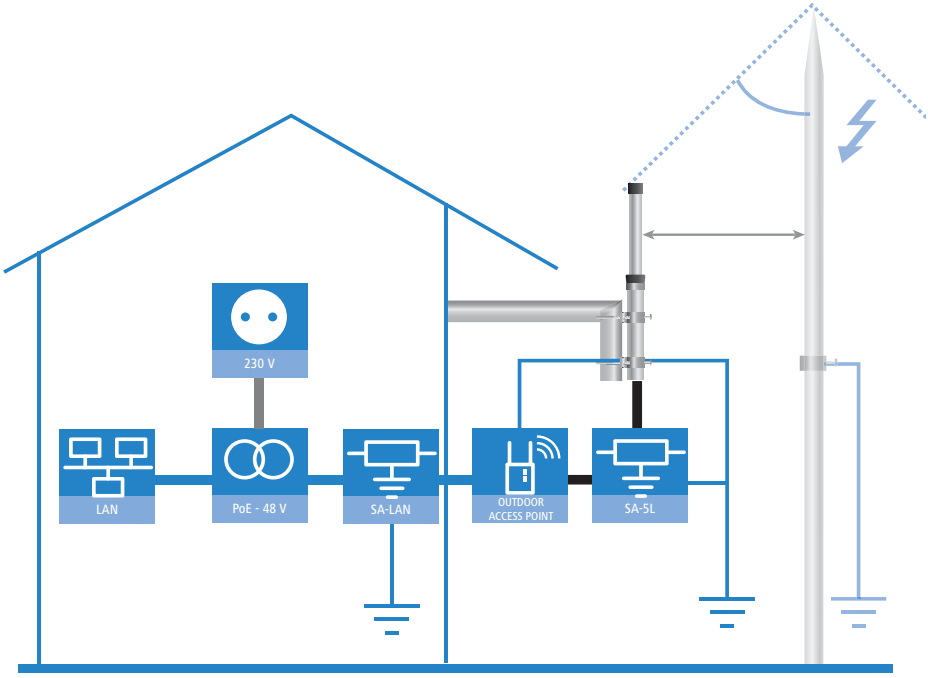


4.3 Internal lightning protection

Internal lightning protection refers to measures which counteract the effects of lightning strikes and surges that may arise despite the external lightning protection. These disturbances may for example be triggered when a lightning strike some distance away is subsequently diffused through the power network or by discharges in the atmosphere that are not accompanied by visible lightning.
There are two ways in which these surges can get into a building and then spread: Via the connection to the public power supply or via cable entry points, for example antennas fixed to the outside of the building.
The following is a description of how to protect the system form the perspective of antennas. Protection for equipment connected to the power supply from surges emanating from the public power supply must be planned and implemented by a specialist electrician.



The central component for internal lightning protection is the BAT surge arrestor surge adapter. The employment of the BAT surge arrestor is ***essential under all circumstances***—despite outer lightning-protection measures, partial discharges can still give rise to surges that can damage sensitive WLAN modules.
The BAT surge arrestor is always mounted between the access point and the antenna, preferably as near as possible to the antenna. If the access point is installed outside, its grounding and that of the BAT surge arrestor are connected with the antenna's conductor, for example via the clamps on the antenna's mounting.
In addition to this, an LAN surge adapter can also be used to reduce possible surges in the ethernet or PoE cable.



4.3.1 Selecting the lightning and surge protective components

Classification of surge protective devices

So-called surge protective devices (SPDs) are used to protect electrical and electronic devices in buildings. These are divided into various categories depending on the purpose of their application:

- ***Buildings***: The biggest danger from the effects of lightning strikes lies in the transmission of lightning current over the cables leading from exposed objects such as antennas directly into the building. So-called lightning arresters (type 1) offer protection from these lightning currents. They are fitted to the relevant cables directly where they enter the building. This type of lightning protective device prevents lightning current from entering via the protected cabling – however, surges can still occur that must be prevented through the use of further surge protection adapters (e. g. BAT surge arrestor).
- ***Power supply***: Surges can also find their way into the building via the power supply and thereby endanger electronic equipment. Surge arresters (type 2) can be used to protect against such surges. They work by reducing the voltage peaks to a sufficiently low level. These type 2 adapters are fitted for example in the electrical cabinet.
- ***Devices***: The final link in the surge protective chain is the protection of the devices themselves. For this, type 3 surge protective devices are used, for example in the form of power socket adapters. This type of SPD works by lowering any surges that may occur to a level that is not dangerous for highly sensitive equipment.

The assessment of risk and the resulting design of a suitable lightning protection system is always dependent on local conditions (for example the frequency with which lightning strikes are to be expected) and ideally needs to be carried out by trained experts.

Caution: Please note that in addition to implementing lightning protection for wireless LAN systems, protection must be separately planned and installed for the building itself and for other equipment.

The following considerations are intended to assist with planning the components to use:

External lightning protection

- Lightning rod
  - ***When?*** Required if the antenna or any other element of the wireless LAN system is mounted in an exposed position.
  - ***Where?*** At least 50 cm safety clearance to the antenna or other conductive element of the wireless LAN system, and preferably more than 100 cm.
  - ***Conductor?*** Grounding via potential equalization line (PEL, 16 mm² Cu) is always required.

Danger: If the safety clearance is less than 100 cm the grounding of the lightning rod must be connected with the grounding of the antenna.

- Antenna potential equalization
  - ***Separate conductor:*** Via separate potential equalization line (PEL, 16 mm² Cu) if there is no lightning rod present (antenna not installed in an exposed position).
  - ***Separate conductor:*** Via separate potential equalization cable (16 mm² Cu) if the safety clearance between the the lightning and the antenna is more than 100 cm.
  - ***Via lightning rod conductor:*** Grounding via the existing potential equalization cable of the lightning rod when the safety clearance between lightning rod and antenna or other conductive element of the wireless LAN system is more than 50 cm but less than 100 cm.

Internal lightning protection

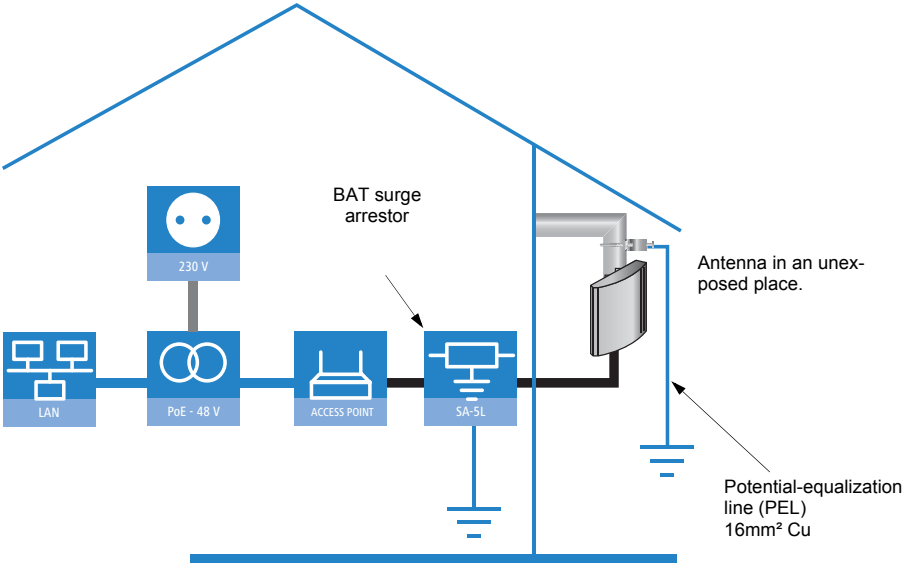
- Surge-protection adapter BAT surge arrestor
  - ***When? Always required.*** Also protects against partial discharges that can damage sensitive wireless LAN modules when there is no direct lightningstrike.
  - ***Where?*** Position as near as possible to antenna connector on the access point.
  - ***Conductor?*** Potential equalization via the building's grounding system using a PE line (protective earth – 1.5 mm² Cu).
- LAN surge adapter
  - ***When?*** Required to protect LAN cabling and equipment.
  - ***Where?*** As near as possible to the access point's ETH connector.
  - ***Conductor?*** Potential equalization via the building's grounding system using a PE line (protective earth – 1.5 mm² Cu).

4.3.2 Example applications

Depending on where the access points, antennas and lightning rods are positioned there are numerous combinations of lightning and surge protective equipment. The following illustrations show some sample scenarios that are frequently found in practice. With this knowledge you will be able to put together the components required for other constellations.

Scenario 1:

Antenna in an unexposed place.

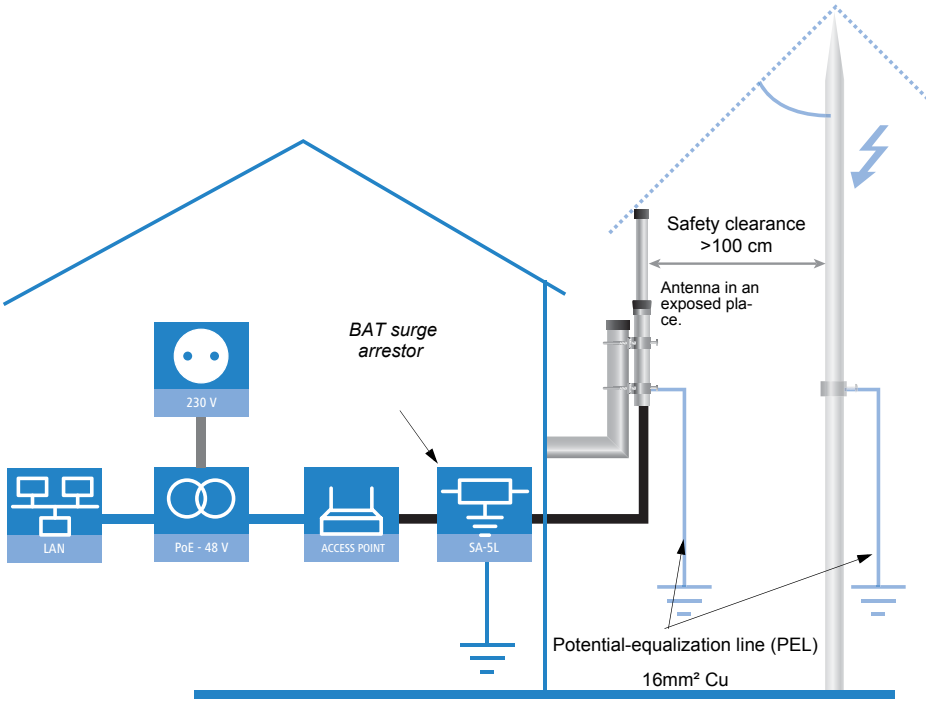


The basic situation shows an application where the antenna is not mounted in an exposed place – there is therefore no danger of a direct lightning strike.

- It is sufficient for lightning protection to have an adequately dimensioned potential equalization line for the antenna.
- The access point must be protected with a BAT surge arrestor for internal protection in any case.

Scenario 2:

Antenna in an exposed place, safety clearance to arresting device observed.

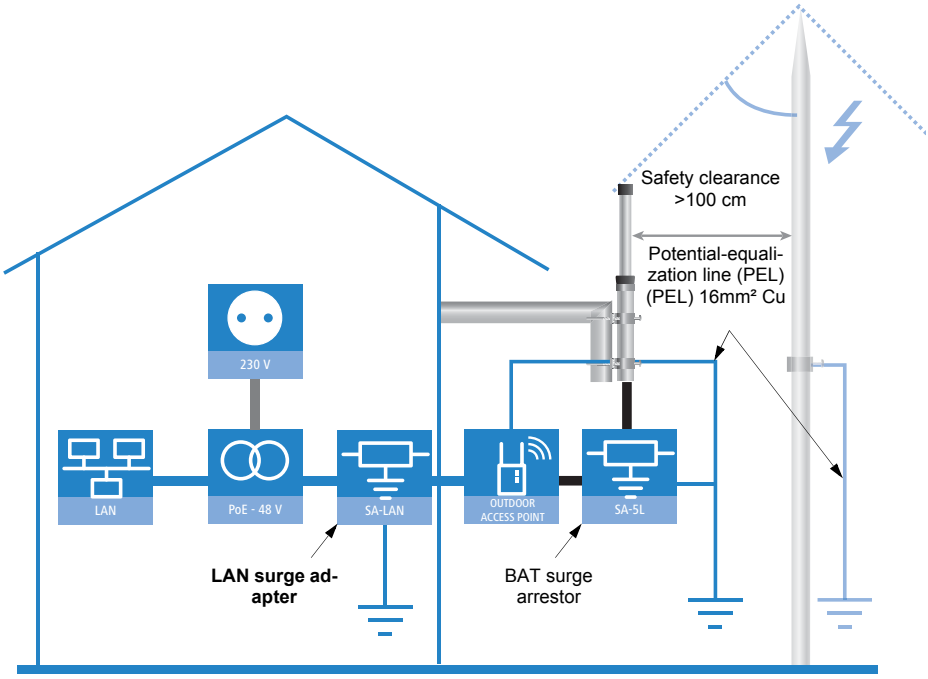


In this example the antenna is mounted in such a way that a direct lightning strike is possible. A lightning rod with a sufficiently large safety clearance of more than 100 cm is installed as a protective measure.

- As external lightning protection both the antenna and the lightning rod are separately grounded with their own potential equalization lines.
- There are no other aspects to be considered for internal lightning protection.

Scenario 3:

The access point is not installed inside the building but outdoors, for example directly next to the antenna, in order to reduce the length of cable between the antenna and the access point.



In this case, the BAT surge arrestor surge-protection adapter is installed directly between access point and antenna and grounded for example via the antenna's potential equalization line.

- If the access point is installed outside, its grounding and that of the BAT surge arrestor are connected with the antenna's conductor, for example via the clamps on the antenna's mounting.
- The BAT surge arrestor can be fixed directly to the antenna socket, depending on the model of the access point.

5 Installation

5.1 Safety advice

Danger: Do not mount access points or antennas in weather conditions when lightning may be expected.
Similarly, refrain from connecting or disconnecting cables during weather of this type.
The components of a wireless LAN can be subject to variations in electrical charge even in normal weather conditions. Please perform all work with the utmost care.

Note: access points, antennas and mounting equipment such as masts intended for outdoor operation must be grounded. Never work with access points and antennas if you are not certain of proper ground. Please seek advice from a qualified electrician to clarify this issue.

The installation and mounting of access points and antennas should only be carried out by experienced IT personnel or trained electricians. Please observe the following notices to avoid accidents:

- Never carry out work of this type alone, but with a minimum of two people. This ensures that help can be quicker to hand if an accident occurs despite all safety precautions.
- Only use ladders with the appropriate insulation.
- Do not work in strong winds or rain.
- Wear suitable working clothing, such as close-fitting clothing and safety shoes with non-slip soles.
- If components of the antenna or mountings should be dropped, let them fall and do not attempt to catch them. Falling antennas, masts or cables may come into contact with live contacts and cause electric shock.
- The mounting location should be easily accessible in the interests of future maintenance work or for checking cable connections.
- Before commencing with mounting, ensure that you have all the necessary tools and accessory parts. Similarly, ensure that any openings required for the entry of the coaxial or Ethernet cable into the building are already available.

Danger: In the interests of your own safety, antennas, masts and the grounding system should only be installed by experienced electricians who are familiar with local conditions and any legal regulations which apply. Furthermore, please observe the notices in section → 'Surge and lightning protection' and ensure that the grounding system meets requirements.

5.2 Mounting the access points

The method for mounting the access point depends on the model's design. This section presents the various mounting types as illustrated by examples. Please refer to the documentation of the relevant access point for more precise instructions.

Caution: Please observe the following advice during installation:
access points installed outside may ***only*** be protected from direct lightning strikes with a lightning rod with a safety clearance of ***more than 100 cm***.
access points installed outside must be grounded with an adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² CU.
The BAT surge arrestor must be used to protect sensitive wireless LAN modules.

5.2.1 Selecting where to mount

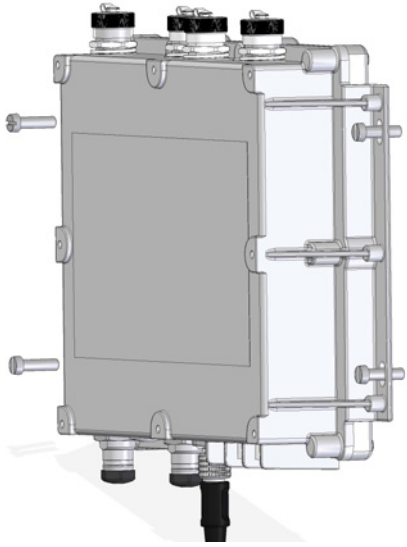
Before mounting any access points a suitable location should be found that meets the following conditions:

- The access points and antennas should not be covered up in order to avoid interference or overheating etc. during transmission and reception.
- Choose a location that is as close as possible to the necessary connections such as LAN interfaces or power sockets.
- Position the access points as close as possible to the antennas. The length of the coaxial cable between access point and antenna has a considerable influence on the attenuation in the wireless LAN system as a whole, thus impacting the available range and data rates, for example.
- Maximum separation is also important for an access point and PoE injector. Some access points have for example an increased power requirement that can only be supplied over a specific length of ethernet cable. Detailed advice is available in the documentation for the access point or the PoE injector.

- Locations where components are mounted outdoors should be as close as possible to the point where the coaxial or Ethernet cables enter the building. Excessive stretches of outdoor cabling are exposed to increased danger from the effects of lightning.
- Avoid locations that are very dusty.
- In outdoor areas, avoid locations that are close to exposed metallic conductors such as guttering, downpipes, etc.

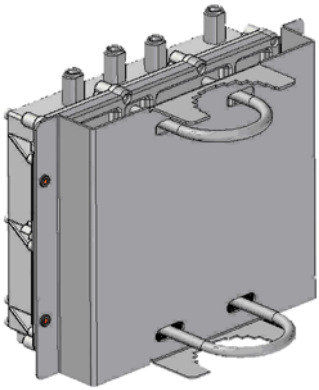
5.2.2 Wall mounting

Wall mounting is an option for all access points and is a suitable method when the intended antenna location is not too far removed.



5.2.3 Pole mounting

If the distance separating the wall-mounted access point and the antenna is likely to end up being too large, the access point can alternatively be affixed in the immediate vicinity of the antenna, for example on a mast or similar arrangement.



5.3 Mounting antennas

The method for mounting the antenna depends on the model's design. This section presents the various mounting types as illustrated by examples. Please refer to the documentation of the relevant antenna for more precise instructions.

Caution: Please observe the following advice during installation:
Antennas mounted outside in an exposed location where direct lightning strikes can occur must be protected by a lightning rod installed at a distance of at least 100 cm.
Antennas mounted outside must be grounded with an adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² Cu.
The BAT surge arrestor must be used to protect sensitive wireless LAN modules.

5.3.1 Selecting where to mount

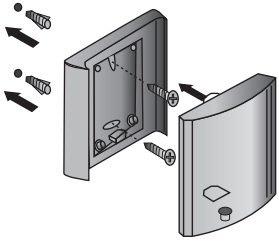
Before mounting any antennas a suitable location should be found that meets the following conditions:

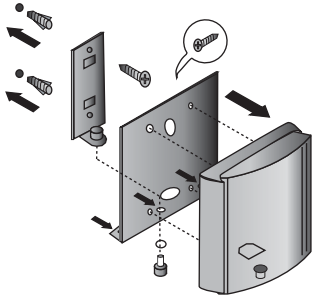
- Mount the antennas in a place offering a good line of sight for transmitting data to mobile wireless LAN clients or remote P2P stations. You will find advice on antenna alignment in P2P mode in Chapter → 'Point-to-point connections (P2P mode)'.

- Mount antennas as near as possible to the access points. The length of the coaxial cable between access point and antenna has a considerable influence on the attenuation in the wireless LAN system as a whole, thus impacting for example the available range and possible data rates.
- Locations where components are mounted outdoors should be as close as possible to the point where the coaxial or Ethernet cables enter the building. Excessive stretches of outdoor cabling are exposed to increased danger from the effects of lightning.
- In outdoor areas, avoid locations that are close to exposed metallic conductors such as guttering, downpipes, etc.

5.3.2 Wall mounting

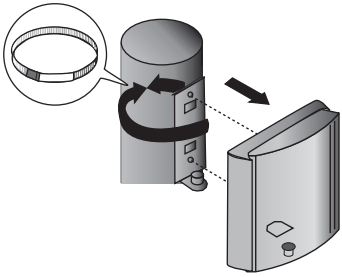
Permanent mounting can take place directly on a wall or with the adjustable swivel fixture.

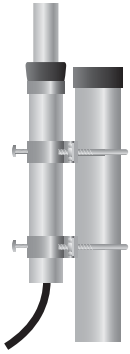




5.3.3 Mast mounting

An alternative is to mount the antenna directly on a mast or similar, thus ensuring that the antenna has a particularly high degree of exposure.





5.4 Mounting the lightning rods

Lightning rods create a spatial shield that is designed to protect the components in a wireless LAN such as antennas or access points from a direct lightning strike.
The following aspects should be considered when choosing where to mount them:

- Dimensioning of the lightning rod
- Vertical and horizontal distance from the components at risk
- Lightning rod grounding

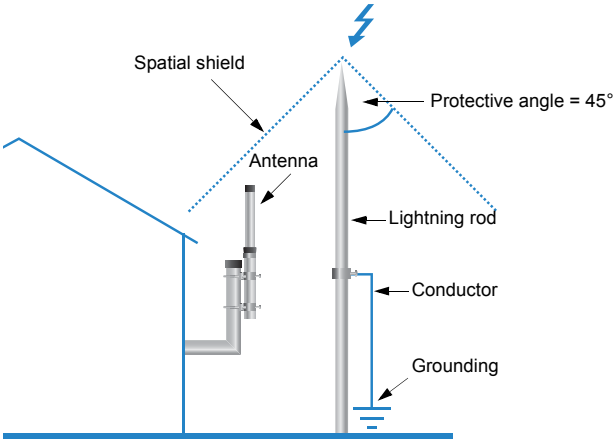
Danger: The dimensioning, installation and grounding of the lightning rods should only be performed by trained electricians.

5.4.1 Dimensioning of the lightning rod

The lightning rod must be able to conduct the complete charge of a lightning strike. For this reason it is important to select rods made from highly conductive metals, for example copper alloys or steel. It is important to select rods with a cross-section that allows the lightning charge to be conducted without being damaged, in general a diameter of between 10 and 16 mm.

5.4.2 Distance to the components at risk

The height and the safety clearance of the lightning rod to the equipment to be protected (e. g. antenna) are used to dimension the lightning rods for a sufficiently large spatial shield.



- Distance of the lightning rods from the antenna: Positioning the lightning rod a sufficient distance away from the antenna prevents the conducted lightning charge from flashing over to the antenna or other conductive components. This distance can be calculated exactly on the basis of several factors. However, in practice a safety clearance of more than 100 cm is generally sufficient.

Note: The distance between lightning rod and antenna has a direct influence on the grounding required by the components. Please observe the advice about grounding the lightning rods and grounding the antennas and access points.

- Lightning rod height: The lightning rod must be high enough to ensure that the equipment that is to be protected such as antennas are within the spatial shield. Besides the exact rolling sphere method used to determine the areas at risk there is the simpler protective angle method which can be used to approximate the spatial shield formed by a lightning rod. This method assumes an area of 45° under the lightning rod to be safe from direct lightning strikes.

5.4.3 Lightning charge conduction (grounding)

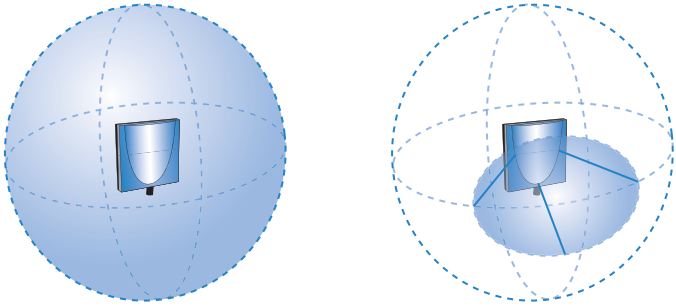
Lightning rods must always be grounded with a separate, adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² Cu. The connection to the grounding system must be made using the shortest path.

Note: If the lightning rod and antenna are mounted together on the same mast and the distance to the antenna is more than 100 cm, the lightning rod must be adequately insulated from the mast since in this case the lightning rod and the antenna must be separately grounded.

6 Appendix

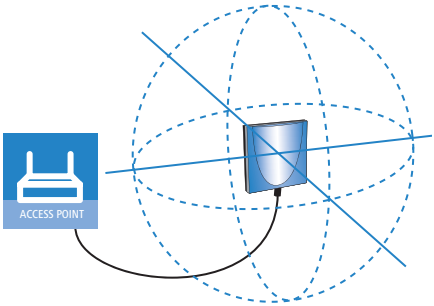
6.1 Antenna gain, EIRP and antenna radiation characteristics

In order to be able to make a statement on the suitability of an antenna for any particular application, the technical specifications state data such as antenna gain, radiated power (EIRP), angle of beam spread, and the radiation characteristics of the antenna.
In practice, the different antenna models have beams that are focused into sectors of varying size. These geometrical radiation characteristics are expressed by the equivalent isotropic radiated power, or EIRP. To determine EIRP, an antenna is viewed theoretically as an isotropic or spherical radiator that emits radiation of the same power in all directions. The EIRP is the amount of power that would have to be emitted by an isotropic antenna to produce the peak power density observed in the direction of maximum antenna gain.

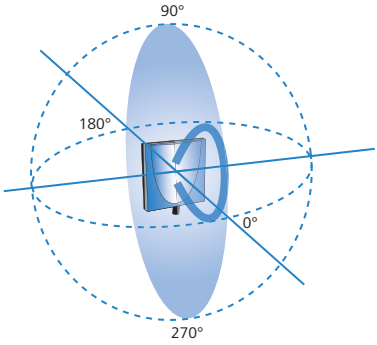


The power fed into the antenna is focused, and thus amplified, into a main beam direction. This amplification is referred to as "gain". The greater the focussing, the greater is the antenna gain.

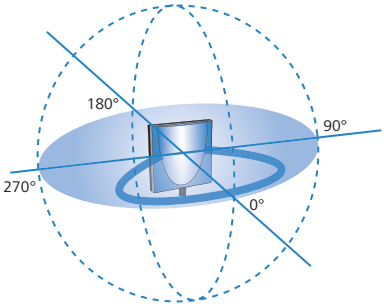
The geometrical beam pattern from an antenna is described by the angle of beam spread and by what is referred to as the radiation characteristics. The radiation characteristics represent the spatial distribution of the radiated power.



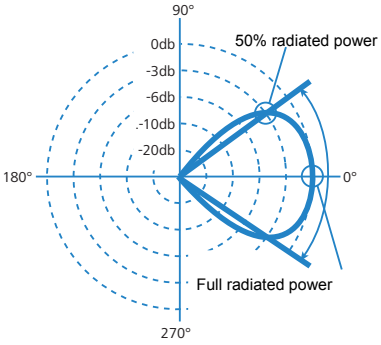
To simplify the problems of representing three-dimensional power distribution, two planes (horizontal and vertical) are taken and the emitted power is plotted as measured in various directions.



The bold line indicates the power that was measured in a certain direction. If this line reaches the outer limit of the "ideal radiation sphere", then the maximum antenna power is radiated in this direction. The closer the bold line comes to the center of the sphere, the lower the radiation emitted in that direction is.



These radiation characteristics are generally transferred onto paper for convenience. The horizontal radiation characteristics may appear for example as follows, :



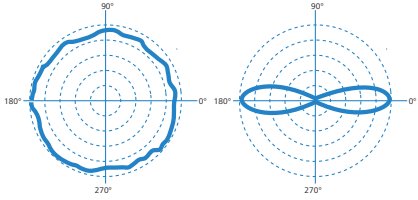
We can see that power in the horizontal direction is strongest directly in front of the antenna (0°). Within the beam angle shown here, power levels are down to just half of the maximum power. This angle is delimited by the points where the power line intersects the -3dB line, which defines a reduction in power by 50%. The other lines indicate a drop from maximum power by -6 dB, -10 dB, and -20 dB. The angle between the two directions where power drops to just 50 % of the maximum is referred to as the 3dB angle or the "half-power width".

For many applications, this angle describes the antenna beam width that can be used in practice. Because this 3 dB angle can differ greatly between the horizontal and vertical planes, these are stated separately in the technical specifications for an antenna. If just one angle is stated, then generally speaking the angles in the two planes will be the same.

Note: The radiation characteristics do not indicate absolute transmission power or transmission range. It merely serves to indicate the percentage of maximum power that is emitted in any given direction.

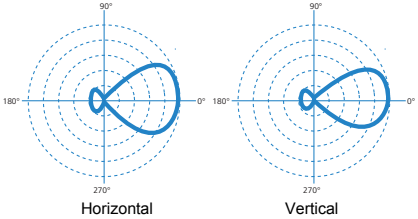
Example applications of various wireless LAN antennas

- Omnidirectional antennas transmit horizontally with equal power in all directions. They have very limited vertical spread, which determines the antenna gain. Antennas of this type are typ ically located in the center of larger offices to provide even coverage to all clients. However, the client adapters should all be at a similar height to receive the best signal from the central antenna.



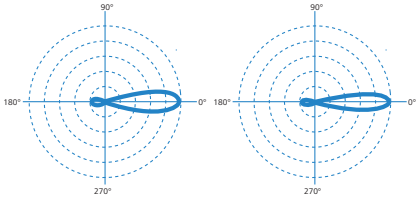
Omnidirectional antennas typically have an low antenna gain of 2 to 4 dBi, for example.

- Sector antennas have beams with fairly wide horizontal and vertical angles, for example between 60° and 90°. Sector antennas are generally mounted on the wall of a building or in the corner of a room to provide an even coverage—often referred to as "campus coverage".



Standard sector antennas have a medium an tenna gain of between 8 and 9 dBi.

- Directional antennas have beams with narrow horizontal and vertical angles, for example of 9°. Directional antennas are mainly used on rooftops or masts for establishing point-to-point links that interconnect areas of a network that are separated by a distance.



  Directional antennas achieve very high antenna gains, sometimes exceeding 20 dBi. Most models are suitable for operating either at 5 GHz or 2.4 GHz only.

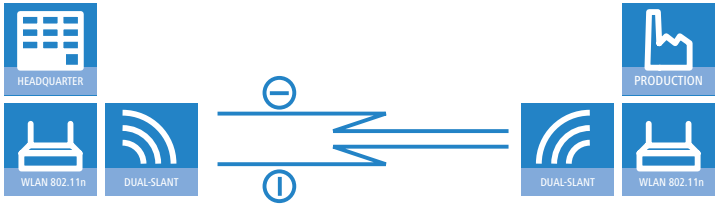
Note: These examples illustrate the tendency for smaller beam widths to result in larger antenna gains. Apart from the focusing effect, the size of the antenna also contributes to antenna gain: Larger antennas ge nera lly result in better antenna gain.

- Polarization diversity antennas (antenna diversity)
  The transmission of radio signals can suffer from, among other things, significant signal losses due to reflection and scatter . When electromagnetic waves overlap at the point of reception, the strength of the signals may be reduced or completely obliterated (interference). Transmission quality can be improved with so-called "diversity" methods.
  The polarization diversity method makes use of the electromagnetic polarization of the radio waves. The transmitter broadcasts the wireless LAN signals as linearly polarized waves with a fixed direction of polarization. The polarization may be modified over the radio link by reflection and diffraction so that signals reach the receiver with differing polarization. Polarization diversity antennas use two signals with a relative polarization of, for example, precisely 90°. The combination of the two signals results in higher antenna gain. Two antennas are connected to the access point's main and auxiliary ports in order to receive both signals.

Note: Weitere Informationen zum Thema ’Polarization diversity antennas (antenna diversity)’ finden Sie im LCOS Referenzhandbuch.

- Polarization diversity with access points in accordance with IEEE 802.11n access points according to IEEE 802.11n make use of MIMO technology (multiple input, multiple output) to transmit data. With this method, several antennas are used to transmit and receive data simultaneously.

For point-to-point connections with appropriate access points and antennas it thus is possible to realize two parallel data connections between transmitter and receiver. A "dual-slant" antenna is connected to two antenna sockets on the access point. One connection is then transmitted with horizontal polarization while the other is transmitted with vertical polarization. Combining the two connections allows significantly higher data transfer rates to be achieved than with previous wireless LAN standards.



6.2 Selecting the frequency band

6.2.1 2.4 or 5 GHz band

One of the first steps in the planning of a wireless LAN system is to determine which frequency band is to be used. The following aspects are helpful for decision making:

- Advantages of the 2.4 GHz band
  - Simple technical implementation with no need for functions such as TPC or DFS.
  - Widespread wireless LAN client base.
- Disadvantages of the 2.4 GHz band
  - Frequency band is also used by Bluetooth, microwave ovens, etc., i.e. prone to interference.
  - There are only three non-overlapping channels, meaning that only three networks can be operated in parallel without interference.
- Advantages of the 5 GHz band
  - The frequency band is not heavily used, so that interference from other applications is uncommon.
  - 19 non-overlapping channels, i.e. several parallel networks can be operated without interference.

- High ranges due to power levels of up to 1000 mW.

- Disadvantages of the 5 GHz band
  - Regulations in Europe demand techniques such as DFS for channel selection and TPC for power control.
  - Small wireless LAN client base.

Note: In general we can assume that WLAN systems based on the 2.4-GHz band are best suited to applications where WLAN clients need short-range connection to an access point (campus coverage, hotspots, data transfer to mobile objects). The advantages of the 5 GHz band lie mainly with point-to-point systems, whereby two access points are connected by a wireless link over longer distances.

6.2.2 Special regulations for the 5 GHz band

With the 802.11h enhancement of September 2003, the private use of the 5 GHz band was finally possible even outside closed spaces. To protect military applications in the 5 GHz band, the DFS (Dynamic Frequency Selection) and TPC (Transmission Power Control) procedures were prescribed. However, DFS and TPC allow significantly higher transmission powers (maximum 1000 mW) to be used than with other previously valid standards.

- Dynamic Frequency Selection – DFS
  Dynamic Frequency Selection (DFS) was stipulated to prioritize primary applications. DFS initially assumes that no channel is available in the corresponding frequency band. The wireless LAN device initially selects an arbitrary channel and performs what is known as a Channel Availability Check (CAC). ***Before*** transmitting on a channel for 60 seconds (Channel Observation Time, COT), a check is run to see if a different device is already working on this channel and the channel is therefore occupied. If this is the case a different channel is checked by the CAC. If not, then the wireless LAN device can start transmitting.
  Even during operation a check is run to see if a primary application such as a radar device is using this channel. This exploits the fact that radars frequently work according to the rotation method, whereby a tightly bundled directional transmission signal is transmitted by a rotating antenna. A remote receiver perceives the radar signal as a short pulse (radar peak). If a device receives such a radar peak, then it pauses the transmission operation and monitors the channel for further pulses. If additional radar peaks occur during the COT, then a new channel is selected automatically.

Caution: The connection can now be operated for any length of time on the channel selected by the DFS algorithm until either a radar signal is detected or the radio cell is restarted (e. g. by changing the device configuration, firmware upload, or restart).

DFS is stipulated for the frequency ranges from 5250 - 5350 MHz and from 5470 - 5725 MHz. It is optional for the frequency range of 5150 - 5250 MHz.

- Transmission Power Control – TPC
  Dynamic adjustment of the transmission power is intended to reduce radio interference.
  Dynamically adjusting the transmission power makes it easier for the 5250-5350 MHz and 5470 - 5725 MHz frequency bands to be shared with satellite services. TPC is designed to cause an average reduction in the transmission power by at least 3 dB compared with the maximum permitted transmission power. TPC determines the minimum transmission power necessary to maintain the connection with the partner (such as an access point). If TPC is not used within these frequency bands, then the highest permissible average EIRP and the corresponding maximum EIRP density are reduced by 3 dB. This restriction does not apply to the frequency range of 5150 - 5350 MHz.
  Without DFS and TPC, a maximum of only 30 mW EIRP is permitted. When DFS and TPC are used, a maximum 1000 mW EIRP is permitted as the transmission power (compared with 100 mW for 802.11 b/g, 2.4 GHz, DFS and TPC are not possible here). The higher maximum transmission power not only compensates for the higher attenuation of 5 GHz radio waves in air, it also makes significantly longer ranges possible than in the 2.4 GHz range.

Available channels in the 5 GHz band

In the available frequency range of 5.13 to 5.805 GHz, up to 19 channels are available in Europe, divided into frequency ranges for which different conditions of use may apply:

- 5150 -5350 MHz (channels 36, 40, 44 and 48)
- 5250 -5350 MHz (channels 52, 56, 60 and 64)
- 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140)
- Band 3: 5725 - 5875 MHz (channels 147, 151, 155 and 167)

The following overview shows which channels may be used in the different regions.

Channel	Frequency	ETSI (EU)	FCC (US)
36	5,180 GHz	yes	yes
40	5,200 GHz	yes	yes
44	5,220 GHz	yes	yes
48	5,240 GHz	yes	yes
52	5,260 GHz	yes	yes
56	5,280 GHz	yes	yes
60	5,300 GHz	yes	yes
64	5,320 GHz	yes	yes
100	5,500 GHz	yes	no
104	5,520 GHz	yes	no
108	5,540 GHz	yes	no
112	5,560 GHz	yes	no
116	5,580 GHz	yes	no
120	5,600 GHz	yes	no
124	5,620 GHz	yes	no
128	5,640 GHz	yes	no
132	5,660 GHz	yes	no
136	5,680 GHz	yes	no
140	5,700 GHz	yes	no
147	5,735 GHz	yes *	no
149	5,745 GHz	no	yes
151	5,755 GHz	yes *	no
153	5,765 GHz	no	yes
155	5,775 GHz	yes *	no
157	5,785 GHz	no	yes
161	5,805 GHz	no	yes
165	5,825 GHz	no	yes
167	5.835 GHz	yes *	no

Note: * Note: Please note that the frequency ranges and radio channels in band 3 are subject to certain restrictions depending on country (e.g. in Germany only permitted for public "Broadband Fixed Wireless Access" communications providers).

Frequency ranges for indoor/outdoor use in the 5 GHz band

The use of the methods described in ETSI 301 893 for reducing mutual interference in the 5 GHz band (TPC and DFS) is not stipulated for all fields of application. The following table provides information about the permitted use and corresponding transmission powers within the EU:

Frequency (GHz)	Transmissionpower (mW/dBm)	Use	DFS	TPC
5,15-5,25	30/13	Indoor		
5,15-5,25	60/14	Indoor		✔
5,15-5,25	200/23	Indoor	✔	✔
5,25-5,35	200/23	Indoor	✔	✔
5,470-5,725	4000/36	Indoor/Outdoor	✔	✔

Note: Other regulations may apply for use in other countries. Please refer to the current wireless network regulations for the country in which you wish to operate a wireless LAN device, and ensure that you set the country of operation in the wireless LAN settings.

The USA and Asia use different frequency bands and maximum signal strengths that are different than the European standard.
In the USA, three subbands, each 100 MHz wide, are used for wireless networks in the 5 GHz band. The "lower band" ranges from 5150 - 5250 MHz, the "middle band" ranges from 5250 - 5350 MHz and the "upper band" ranges from 5725 - 5825 MHz. In the lower band, a maximum average EIRP of 50 mW is permitted; in the middle band this is 250 mW and 1 W in the upper band.
In Japan, the use of the 5 GHz band is possible to a limited extent: only the lower band of 5150 - 5250 MHz is approved for private use.

7 Index

Numerics
2.4-GHz band
Advantages 45
Disadvantages 45
5-GHz band 47, 49
Advantages 45
Disadvantages 46

A
Access point 11
Angle of beam spread 41
Antenna Calculator 16
Antenna diversity 13, 44
Antenna gain 40
Antenna power 18

C
Campus coverage 7

D
Data communication to mobile objects 8
DFS 16, 46, 49
Directional antenna 13, 44
Download 6
Dynamic Frequency Selection 16, 46
Dynamic frequency selection 16

E
EIRP 40, 47
Equivalent isotropic radiated power 40

F
Firmware 6
Fresnel zone 18

G
Gain 40

H
Hotspot 8

I
IEEE 802.11a 12
IEEE 802.11b 12
IEEE 802.11g 12
IEEE 802.11n 12
Industrial applications 8
Isotropic radiator 40

L
Lightning protection
Designing the lightning protection system 26
Internal lightning protection 25
Surge-protection adapter SA-5L 28, 30, 31, 32
Lightning protector
External lightning protection 24
Lightning current arresters 24
Lightning rods 24
Lower band 49

M
Middle band 49
Mounting access points
Pole mounting 35
Wall mounting 35
Mounting antennas
Pole mounting 37
Wall mounting 37

O
Omnidirectional antenna 13, 43

P
PoE 12
PoE Injector 12
Point-to-multipoint 9
Point-to-point 9
Point-to-point mode 15
Polarization diversity 14, 44
Power hub 12
Power over Ethernet 12
Power supply 12
Power switch 12

R
Radiation characteristics 40
Radio channels
Indoor and outdoor operation 49
Radio channels ETSI (EU) 48
Radio channels FCC (US) 48
Relay mode 11

S
Safety advice 33
Sector antenna 13, 43
Support 6

T
TPC 46, 47, 49
Transmission Power Control 47

U
Upper band 49
User group 8

W
Wireless router 11